Mission Assurance: Analysis for Cyber Operations

21 –24 March 2011
Southwest Research Institute
San Antonio, TX

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **MAR 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE
Working Group 3: Operate and Defense Network

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army Test and Evaluation Command,4501 Ford Ave,Alexandria,VA,22302-1458

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
MORS Mission Assurance: Analysis for Cyber Operations Special Meeting held in San Antonio, TX Mar 21-24, 2011.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

Mission Assurance: Analysis for Cyber Operations

21 –24 March 2011 | Southwest Research Institute | San Antonio, TX

Working Group 3: Operate and Defense the Network

Ken Christy (MITRE/PACOM)
Pat Thompson (ATEC)

Purpose

- Understand the significant challenges to Cyber Mission Assurance as it relates to operating and defending the DOD network.

- Understand how Operations Research Analysis can assist the achievement of Cyber Mission Assurance as it relates operating and defending the DOD network.

Overall Observations

- The cyber community needs to understand Operations Research capabilities
  - Consider sharing MORS documents on SIPRNET, JWICS, and NSANet (Intellipedia and IntelDocs are easy ways to start)
  - Institutionalize cross flow of information across these communities
  - More MORS outreach to cyber community ("cyber") conferences and workshops.
    - MORS Cyber Community of Practice?

Issues

1. Issue: How do you measure mission assurance?
2. Issue: Centralized planning vs. decentralized command and control
3. Issue: Lack of doctrine standardization inhibits both communication and C2
4. Issue: Cyber Workforce Structure
5. Issue: Cyber training and certification
6. Issue: Incident handling process*
7. Issue: Supply Chain Vulnerability Risk Management
8. Issue: Social media: is benefit worth the risk?*
9. Issue: Recognition of and Response to internally vs. externally imposed degradations
10. Issue: Evaluation of new and existing sensor technologies, as well as placement within networks, based on mission set.*

* Potential low hanging fruit

Issues (cont.)

11. Issue: Stovepiping of NETOPS, CND, Intelligence, and LE information leads to an inability to share.
12. Issue: Presentation of Forces
13. Issue: Authorities and Integrated Teams
14. Issue: INFOCON / TRO: need to revise
15. Issue: Multinational Integration
16. Issue: Public / Private Partnerships
17. Issue: What is the best way to coordinate, synchronize, and leverage Electronic Warfare and the "networked" Cyberspace Domain
18. Issue: Cloud computing

Issue: How do you measure mission assurance?

- Discussion:
  - Performance metrics - bandwidth, successful communications, mitigation and recovery
  - What happens when you don't control all of the circuits? Provisioning for failure modes / loss of IAP
  - Network modeling
  - No effective Mission Assurance Analysis
  - Identify critical missions and critical assets (defended asset list)
  - Identify critical assets (links and nodes) mapped to missions
  - Ensure critical assets are defendable (resilient and reliable)
- DOTMLPF: Doctrine, Material
- Analysis Considerations: Develop performance metrics (MOE, MOP). How good is good enough? M&S for mission assurance, based on criticality list. Critical asset mapping

Issue: Centralized planning vs. decentralized command and control

- Discussion:
  - With centralized planning and decentralized execution, who determines MA priorities?
    - How do we map mission(s) to assets (data, application, services, links)?
    - Authority to control (block, limit) access to non-GIG applications
  - OPCON / TACON issues: Concerns over CYBERCOM directing individual units and COCOMs bypassing CYBERCOM. What should be the role of Regional cyber commands?
  - How are COOP / Alternate Operating Locations factored into planning?
- DOTMLPF Areas: Doctrine, Organization, Facilities
- Analysis Considerations: Understanding tradeoffs and risk. Risk Model: vulnerability and likelihood. A new study to look at regional vs. global command structures

Issue: Lack of doctrine standardization inhibits both communication and C2

- Discussion: Impact to training and to development of Joint / Multiservice capabilities to achieve interoperability and fusion for joint force commanders.
- DOTMLPF Considerations: Doctrine, Training, Material
- Analysis Considerations: Functional decomposition of cyber "operate" and "defend" missions, mapped to Joint and Service doctrinal terms. Analysis of impact to training and material development.

Issue: Cyber Workforce Structure

- Discussion: Technical advancement / career path for services (warrant officers / LDO). How to most effectively use limited personnel (might drive systems development). How are METLs being used to drive force structure at each command level? How is this tied into SORTS/DRRS rating for cyber capability? What is the right balance between DOD civilian, military, and contractors for the cyber work force? Recruiting & Retention (esp. of junior personnel) Retention can be problematic as junior personnel earn certifications and gain experience. Effectiveness of retention bonuses vs. retraining / replacement. Phasing out retention bonuses after members are well vested. Compensation comparison with equivalent industry positions. Mission accomplishment / contribution are key job satisfaction criteria
- DOTMLPF Considerations: Personnel
- Analysis Considerations: Manpower and compensation analysis

Issue: Cyber training and certification

- Discussion: Sufficiency of DODI 8570 (IA Work Force Improvement Program) training/certification for cyber roles; not all roles would need the same training. How does this apply to USAF "Combat Mission Ready" (CMR)? Different requirements for military? Contractors? Government civilian personnel?
  - Appropriate Training Methods. Schools, CBT, ranges (IO, IA), simulation, exercises. Which is the most effective combination? Training to maintain currency / refresher training
  - Lack of joint training standards. Can we establish executive agency for cyber work force training and eliminate redundancy across the Services.
  - Joint Cyber Training Centers need to be available and geographically dispersed. Include existing tools used across the Services and Agencies
- DOTMLPF: Training, Personnel, Facilities
- Analysis considerations: Determine appropriate mix of training / certification / experience. What is the relevancy of 8570 training to force operations. Efficiency of training. Identify requirements for joint training standards; manpower study for cyber workforce. Optimize resources to meet CMR. Benefit of training end users, net defenders, system administrators. Optimization of training across these different roles. MOP, MOE for training.

Issue: Incident handling process*

- Discussion: Is process optimal, or does it suffer from inefficiencies/other issues that degrade it. Need to look at process to address handling and feedback (e.g., existing incidents and root cause analysis as feedback loop to inform rest of DOTMLPF). JCD (Joint Cyber incident Database) is the joint repository of incident information. Incident response may require shipping of hard drive / IT systems, lengthening the incident response timeline. Need to consider Shipping of replacement hardware / spares, Processes to expedite shipping, Alternatives to shipping (disk images, etc). Consider user level behaviors which cause mission impact. Develop mitigation strategies.
- DOTMLPF Considerations: Material, Logistics, Personnel
- Analysis Consideration: Determine efficiencies and make recommendations across the DOTMLPF. Can timeline be reduced? Root cause analysis, recommendations to mitigate

Issue: Supply Chain Vulnerability Risk Management

- Discussion: Purchasing and transport of hardware and software in a means that meets cyber / architectural requirements, timeliness, FAR, and ensures supply chain integrity. How do you certify the validity of software and hardware. Lifecycle management: how do you ensure future patches / updates are also valid / assured. Impact of "just in time" supply chain / spares to SCVRM. Consider use of DOD supply chain for critical components under higher assurance controls. DOD supply chain will analyze MTBF, MTTR use this to select vendors, and maintain control over higher assurance components. Would need to tie into incident management / asset management databases and share across Services. Issues with scale and agility, mitigated by applying this process to "critical components"
- DOTMLPF Considerations: Doctrine, Material, Logistics
- Analysis Considerations: take a piece of this and analyze. Tradeoffs. Costs vs. vulnerabilities. Consider the optimization / tradeoffs between higher assurance cyber components and the mission criticality of the systems / components

Issue: Social media: is benefit worth the risk?*

- Discussion:
  - Benefit: recruiting, PAO, SC, MWR, alternative means of communicating
  - Cost: OPSEC, social engineering, malware, bandwidth
- DOTMLPF Areas: Doctrine
- Analysis Consideration : Quantify risk (cost / benefit)

Issue: Recognition of and Response to internally vs. externally imposed degradations

- Discussion: Network service degradations / outages can occur from "acts of God", self-imposed mis-configurations, and adversary activity. Decision criteria / decision aids. Mechanisms to fine tune responses to attacks or crisis response. Technical / architectural limiting factors to deal with finer tuned responses
- DOTMLPF Consideration: Doctrine, Material, Training
- Analysis Considerations: Pattern recognition of intentional vs. unintentional degradations. Compare and contrast techniques, machine learning. Understand types of incidents, likelihood of event. Techniques to identify intentional vs. unintentional degradation. Analysis of policy, doctrine, architecture to understand authorities for response actions. Analysis of alternatives to understand different approaches for response actions.

Issue: Evaluation of new and existing sensor technologies, as well as placement within networks, based on mission set.

- Discussion: How are sensor signatures and rulesets shared across DOD and industry partners. Data standards for sharing. How can sensors be optimized for CND analysis, to include placement, aperture, type of sensor (NIDS, HIDS, system logs, signature and non-signature based, etc.). Cross queue and integrate sensors and sources of information for CND. Harmonize with the common data model to inform and support data fusion process. M&S to determine sensor effectiveness (both sensor technology and sensor placement)
- DOTMLPF Consideration: Doctrine, Material, Training
- Analysis Consideration: Effectiveness and optimization of sensors.

Issue: Stovepiping of NETOPS, CND, Intelligence, and LE information leads to an inability to share.

- Discussion: Shared Information/data, processes, tools, SA, etc. leading to collaborative understanding and decision making within, to include CNDSP and IC communities. Different organizations look at different objects, events, patterns, signatures, etc. (horizontal sharing). Tailor to user needs at all levels through data fusion. Different organizations with different authorities (NETOPS, Intel, LE) in the same organization to share information. (multi-disciplinary sharing) Integration of Liaison forces (AF COLE, CYBERCOM Cyber Support Element (CSE)). Planners / liaisons are sent forward as battle rhythm accelerates. Need for a Joint Cyber Data Model.
- DOTMLPF: Doctrine, Organization, Training, Material, Personnel
- Analysis Considerations: Organization design issues to enhance multi-disciplinary and horizontal SA. Performance metrics

Issue: Presentation of Forces

- Discussion: Presentation of forces from Services to CYBERCOM and COCOMs. Capabilities vs. organizations. Understand need across COCOMs. Convey to Services. Deconflict portfolio of capabilities offered for CND/Forensics/Counter Cyber
- DOTMLPF: Organization, Doctrine
- Analysis Considerations: which form of Force Presentation (or Force Generation) is more effective? What are the tradeoffs?

Issue: Authorities and Integrated Teams

- Discussion: Appropriate mix of personnel/organizations and authorities into an integrated team (e.g., cyber, law, intel) to bring together operators with different authorities. Integrating the required steps in the required amount of time (process), as well as the organization change issues (authorities, personnel). Timeliness of switching authorities (Streamlining process). LE necessary at every level? Intelligence necessary at every level. Efficiency vs. tailored response. Consider impact to Command Center design. Separate spaces for LE, Intel, NETOPS, coalition partners, other USG personnel, to include Special Access Facilities (SAF)
- DOTMLPF Considerations: Organization, Facilities
- Analysis Considerations: Organizational design. Optimize space for SAF to ensure it can be properly applied

Issue: INFOCON / TRO: need to revise

- Discussion: current INFOCON is outdated. Needs to be revised. Efforts to employ CYBERCON have stalled. Review of INFOCON process needs to involve development of pre-planned responses and checklists to issue TRO. Approval levels may be out dated and need to be addressed. Must include assessment of risk to mission and risk to network.
- DOTMLPF: Doctrine
- Analysis Considerations: Can we do operational risk management for a specific mission set to optimize cost / benefit of proposed INFOCON / TRO

Issue: Multinational Integration

- Discussion: Afghan Mission Network (AMN) is a potential model (hub and spoke, with enclaves from each partner nation). Need to determine optimal methods to handle NETOPS and CND information sharing (e.g., data, TTP, systems). Identify CND standards for each partner network.
- DOTMLPF: Doctrine, Organization, Training, Materials, Personnel
- Analysis Considerations: Identify quality metrics that don't overly burden user--MOEs, MOPs for coalition integration and sharing for NETOPS and CND. How are we providing and how could we provide a better CNDSP capability.

Issue: Public / Private Partnerships

- Discussion: Industry faces many of the same cyber challenges as the military. How is the DOD sharing cyber information among industry partners to enhance Cyber Force Coordination? Creation of releasable signatures from DOD to industry partners
- DOTMLPF: Doctrine, Organization, Training, Material
- Analysis considerations: effectiveness of liaison forces. Optimized number, skills sets.

Issue: What is the best way to coordinate, synchronize, and leverage Electronic Warfare and the "networked" Cyberspace Domain

- Discussion: EW has proven techniques that cyber operations can learn from, since effects appear to be similar. EW and "networked" cyberspace are mutually supporting. Similarity of personnel skills sets. C2 of EW vs. C2 of Cyber. "Free space" vs. "wired space". Consider application of various Signaling techniques.
- DOTMLPF Considerations: Doctrine, Organizational, Material, Training, Personnel
- Analysis Considerations: Analysis techniques to compare / contrast approaches in EW and Cyber domains. Consider this for discussion at the MORSS WG 31 (IO and Cyber)

Issue: Cloud computing

- Discussion: How is the doctrine for Mission Assurance going to keep up as Services / Agencies move to cloud computing? Recent DOD CIO memo directs Services and Agencies to move "something" into "the cloud". Consider risk mitigation by moving non mission critical services to the cloud. Tradeoffs of "on GIG" and "off GIG" cloud services.
- DOTMLPF Considerations: Doctrine
- Analysis Considerations: Cost / benefit analysis. Performance metrics for different types of cloud architectures.

WG3 Contact Information

- WG Chair: Mr. Ken Christy, MITRE / PACOM J81 (kchristy@mitre.org, 808-387-1406)
- WG Co-chair: Mr. Pat Thompson, ATEC (patrick.a.thompson@us.army.mil, 410-306-1466)
- Dr. Rajive Bagrodia, Scalable Network Technologies, UCLA, rbagrodia@scalable-networks.com
- Dr. Rusty Baldwin, Center for Cyberspace Research, AFIT, rusty.baldwin@afit.edu
- Ms. Erika Banks, USSTRATCOM J7, banksens@stratcom.mil
- Lt Col Brian Bassham, 24 AF/A9 christopher.bassham@us.af.mil
- Mr. Bill Bernard, AF/CVR, william.bernard.ctr@pentagon.af.mil
- Mr. Gregory Chapin, MITRE, gchapin@mitre.org
- Mr. John Diaz, AFRL, RHXS, john.diaz@wpafb.af.mil
- Mr. Michael Hartzell, USAFCENT, michael.hartzell@nosc.afcent.af.mil
- Maj Mike Huntsberger, USCYBERCOM J37, mghunsb@nsa.gov
- Mr. Kent Pickett, MITRE, kpickett@mitre.org
- Mr. Marconi Ratonel, Metron, ratonel@ca.metsci.com
- Lt Col Kevin Rook, 624 OC, kevin.rook@us.af.mil
- LCDR Harrison Schramm, NPGS, hcschram@nps.edu
- Dr. Phillip Webb, IDA, pawebb@ida.org